AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

1-44. (canceled).

45. (currently amended) A computer implemented method for server-side execution in support of financial transactions, comprising:

establishing an authentication record in memory accessible by server-side computer resources, in response to communications at a first time from a particular account holder, for a predicted transaction by the particular account holder, the authentication record for the predicted transaction includes a predicted transaction amount, a transaction time parameter, and an authenticated transaction signature for presentation upon execution of the predicted transaction, and sending a message including the authenticated transaction signature from the server-side computer resources to the particular account holder;

establishing an authorization record in memory accessible by server-side computer resources, in response to communications at a second time from a party to a particular transaction, for the particular transaction indicating an actual transaction amount, an actual transaction time and a presented transaction signature, wherein said establishing an authorization record does not require identification of the particular account holder;

reading and processing the authorization record and the authentication record in the server-side computer resources, and if the presented transaction signature in the authorization record matches the authenticated transaction signature in the authentication record for the predicted transaction, the actual transaction amount in the authorization record matches the predicted transaction amount in the authentication record and the actual transaction time in the authorization record matches the transaction time parameter in the authentication record, then sending an authorization message to the party of the particular transaction; and

performing an accounting process, including reconciling the predicted transaction amount and the actual transaction amount in the server-side computer resources, for the particular account holder.

46. (original) The method of claim 45, including:

storing the authentication record in a database including a plurality of authentication records for other predicted transactions.

47. (previously presented) The method of claim 45, wherein the time parameter comprises a time value indicating the first time, when the authorization record was created.

48. (original) The method of claim 45, wherein said matching includes determining whether the actual transaction time falls within a time interval indicated by the transaction time parameter.

49. (previously presented)The method of claim 45, wherein establishing an authentication record includes:

establishing a communication session with the particular account holder;

accepting an account number and an identification number for the particular account holder via the communication session;

accepting the predicted transaction amount via the communication session; and

producing the transaction signature.

50. (original) The method of claim 49, including prompting the particular account holder to supply a combination of digits from a personal identification code, wherein the combination does not include all of the personal identification code.

51. (previously presented) The method of claim 45, wherein establishing an authorization record includes:

establishing a communication session with the party to the particular transaction; and

accepting the presented transaction signature and the actual transaction amount via the communication session.

52. (previously presented) The method of claim 51, including accepting identification of the party via the communication session.

53. (previously presented) The method of claim 52, including maintaining a list of authorized parties, and including determining whether the identification of the party accepted via the communication session indicates a party in the list of authorized parties.

54. (canceled).

55. (previously presented) The method of claim 45, wherein establishing an authentication record includes:

establishing a communication session with the particular account holder;

accepting an account number via the communication session;

prompting the particular account holder via the communication session to supply a static identification number and a dynamically identified combination of digits from a personal identification code, wherein the combination does not include all of the personal identification code;

accepting the predicted transaction amount via the communication session; and

producing the transaction signature and sending the transaction signature to the particular account holder.

56-57. (canceled).

58. (currently amended) A method for managing financial transactions using a computer system arranged for communication with remote devices using communication lines, comprising:

performing a plurality of authentication processes in response to initiations of respective sessions with the computer system by data communications from remote devices, for predicted transactions having predicted transaction amounts and predicted transaction time out intervals by particular account holders, the authentication processes respectively characterized by the steps of:

generating in the computer system requests for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account used for authenticating the account, at least one ~~factor~~ parameter unique to the

account holder for authenticating the account holder and at least two ~~factors~~ parameters related to the predicted transaction including a transaction specific ~~factor~~ parameter and a transaction type identifier unique to the account holder used for authenticating the predicted transaction;

storing a first time-stamped record in memory including the identifier of the account, the at least one ~~factor~~ parameter unique to the account holder, the transaction specific ~~factor~~ parameter, the transaction type identifier and a time parameter as a part of or as data associated with the first record in memory; and

producing a transaction signature as a function of the identifier of the account, the at least one ~~factor~~ parameter unique to the account holder, the transaction specific ~~factor~~ parameter, the transaction type identifier and the time parameter, for presentation upon execution of the predicted transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

performing, in the computer system, a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions, the authorization process for a particular transaction characterized by the steps of

receiving an account identifier, a presented transaction signature, and an actual transaction amount at an actual transaction time associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record in memory for the authorization request for the particular transaction, the record including the received account identifier, the presented transaction signature, the actual transaction amount and the actual transaction time;

processing the second time-stamped record, in response to one of said first time-stamped records with a matching account identifier, to verify that

the presented transaction signature matches the transaction signature associated with said one of said first records, the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records, the actual transaction type matches the transaction type associated with said one of said first records and the actual transaction time is within the predicted transaction time out interval; and

transmitting authorization signals upon successful authorization to one of said remote devices associated with said particular transaction; and

performing, in the computer system, a plurality of accounting processes for the respective transactions subject of authorization processes, including reconciling the predicted transaction amounts and the actual transaction amounts for each transaction of the particular account holders.

59. (previously presented) The method of claim 58, including:

storing the predicted transaction type identifier, the predicted transaction amount, and the transaction signature for a predicted transaction in a database in said memory.

60. (previously presented) The method of claim 58, including storing a predicted transaction time out interval parameter in the database.

61. (previously presented) The method of claim 58, including setting up a time out interval between the authentication process and the authorization process and after creation of a first time-stamped record for a particular account, monitoring the memory to detect creation of a second time-stamped record having a matching account identifier and attempting said authorization process until one of expiration of the time out interval and success of the authorization process.

62. (previously presented) The method of claim 58, wherein the authentication process is further characterized by executing a process in the computer system prompting the particular account holder via the communication lines to supply to the computer system a transaction specific code based on or equal to a combination of alphanumeric characters at certain randomly chosen

alphanumeric character positions in a password, wherein the combination does not include all of the alphanumeric characters in the password.

63. (previously presented) The method of claim 58, wherein the authorization process includes:

at the server, performing a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions characterized by prioritizing pairs of first time-stamped records and second time-stamped records with matching account identifiers according to their time stamps and time out interval parameters.

64. (previously presented) The method of claim 58, including accepting identification of the party at the server.

65. (previously presented) The method of claim 58, wherein the authorization process operates without identification of the particular account holder to the party.

66. (previously presented) The method of claim 58, wherein the authorization process operates with identification of the particular account holder to the party.

67. (currently amended) A financial transaction server, comprising:

a communication interface;

a computer system including memory coupled to the communication interface, the data processing system including resources for managing financial transactions and for communicating using the communication interface with remote devices, including

an authentication process communicating over the communication interface for authenticating a predicted transaction by a particular account holder, including routines characterized by the steps of:

generating in the computer system requests for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account used for authenticating the account, at least one ~~factor~~ parameter unique to the account holder for authenticating the account holder and at least two

~~factors~~ parameters related to the predicted transaction including a transaction specific ~~factor~~ parameter and a transaction type identifier unique to the account holder used for authenticating the predicted transaction;

storing a first time-stamped record in memory including the identifier of the account, at least one ~~factor~~ parameter unique to the account holder for authenticating the account holder, the transaction specific ~~factor~~ parameter, the transaction type identifier and a time parameter as a part of or as data associated with the first record in memory; and

producing a transaction signature as a function of the identifier of the account, the at least one ~~factor~~ parameter unique to the account holder, the transaction specific ~~factor~~ parameter, the transaction type identifier and the time parameter, for presentation upon execution of the predicted transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

an authorization process communicating over the communication interface for authorizing a particular transaction having an actual transaction amount and an actual transaction time, including routines characterized by the steps of:

receiving an account identifier, a presented transaction signature, and an actual transaction amount at an actual transaction time associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record in memory for the authorization request for the particular transaction, the record including the received account identifier, the presented transaction signature, the actual transaction amount and the actual transaction time;

processing the second time-stamped record, in response to one of said first time-stamped records with a matching account identifier, to verify that the presented transaction signature matches the transaction signature

associated with said one of said first records, the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records, the actual transaction type matches the transaction type associated with said one of said first records and the actual transaction time is within the predicted transaction time out interval; and

transmitting authorization signals upon successful authorization to one of said remote devices associated with said particular transaction; and

an accounting process executed in combination with said authorization processes for respective transactions, including reconciling the predicted transaction amounts and the actual transaction amounts for each transaction of the particular account holders.

68. (previously presented) The financial transaction server of claim 67, wherein the data processing system includes a local or remote database storing the first and second time-stamped records.

69. (previously presented) The financial transaction server of claim 67, wherein the data processing system includes a watchdog routine which after creation of a first time-stamped record for a particular account, monitors the memory to detect creation of a second time-stamped record having a matching account identifier and attempts said authorization process until one of expiration of the time out interval and success of the authorization process.

70. (previously presented) The financial transaction server of claim 67, wherein the authentication process includes routines performing a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions characterized by prioritizing pairs of first time-stamped records and second time-stamped records with matching account identifiers according to their time stamps and time out interval parameters.

71. (previously presented) The financial transaction server of claim 67, wherein the authentication process includes a routine prompting the particular account holder via the communication interface to supply to the computer system a transaction specific code based on

or equal to a combination of alphanumeric characters at certain randomly chosen alphanumeric character positions in a password, wherein the combination does not include all of the alphanumeric characters in the password.

72. (previously presented) The financial transaction server of claim 67, wherein the authorization process includes a routine accepting identification of the party at the server.

73. (previously presented) The financial transaction server of claim 67, wherein the authorization process operates without identification of the particular account holder to the party.

74. (previously presented) The financial transaction server of claim 67, wherein the authorization process operates with identification of the particular account holder to the party.

75. (currently amended) An article of manufacture, comprising:

a machine readable storage medium;

a computer program stored on said machine readable medium with resources executable by a computer system for managing financial transactions, including

an authentication process communicating over the communication interface for authenticating predicted transaction by a particular account holder, including routines characterized by the steps of:

generating in the computer system requests for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account used for authenticating the account, at least one ~~factor~~ parameter unique to the account holder for authenticating the account holder and at least two ~~factors~~ parameters related to the predicted transaction including a transaction specific ~~factor~~ parameter and a transaction type identifier unique to the account holder used for authenticating the predicted transaction;

storing a first time-stamped record in memory including the identifier of the account, at least one ~~factor~~ parameter unique to the account holder for

authenticating the account holder, the transaction specific ~~factor~~ parameter, the transaction type identifier and a time parameter as a part of or as data associated with the first record in memory; and

producing a transaction signature as a function of the identifier of the account, the at least one ~~factor~~ parameter unique to the account holder, the transaction specific ~~factor~~ parameter, the transaction type identifier and the time parameter, for presentation upon execution of the predicted transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

an authorization process communicating over the communication interface for authorizing a particular transaction having an actual transaction amount and an actual transaction time, including routines characterized by the steps of

receiving an account identifier, a presented transaction signature, and an actual transaction amount at an actual transaction time associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record in memory for the authorization request for the particular transaction, the record including the received account identifier, the presented transaction signature, the actual transaction amount and the actual transaction time;

processing the second time-stamped record, in response to one of said first time-stamped records with a matching account identifier, to verify that the presented transaction signature matches the transaction signature associated with said one of said first records, the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records, the actual transaction type matches the transaction type associated with said one of said first records and the actual transaction time is within the predicted transaction time out interval; and

transmitting authorization signals upon successful authorization to one of said remote devices associated with said particular transaction; and

an accounting process executed in combination with said authorization processes for the respective transactions, including reconciling the predicted transaction amounts and the actual transaction amounts for each transaction of the particular account holders.

76. (previously presented) The article of claim 75, wherein the resources include a routine for storing the first and second time-stamped records in a local or remote database.

77. (previously presented) The article of claim 75, wherein the resources include a watchdog routine which after creation of a first record for a particular account, monitors the memory to detect creation of a second record having a matching account identifier and attempts said authorization process until one of expiration of the time out interval and success of the authorization process.

78. (previously presented) The article of claim 75, wherein the authentication process includes a routine prompting the particular account holder via the communication interface to supply to the computer system a transaction specific code based on or equal to a combination of alphanumeric characters at certain randomly chosen alphanumeric character positions in a password, wherein the combination does not include all of the alphanumeric characters in the password.

79. (previously presented) The article of claim 75, wherein the authorization process includes routines performing a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions characterized by prioritizing pairs of first time-stamped records and second time-stamped records with matching account identifiers according to their time stamps and time out interval parameters

80. (previously presented) The article of claim 75, wherein the authorization process includes a routine accepting identification of the party at the server.

81. (previously presented) The article of claim 75, wherein the authorization process operates without identification of the particular account holder to the party.

82. (previously presented) The article of claim 75, wherein the authorization process operates with identification of the particular account holder to the party.